IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA

v.

AHMAD 'UMAR AGHA,
a/k/a, "THE PRO,"

and

FIRAS DARDAR,
a/k/a, "THE SHADOW,"

Defendants

Criminal No. 1:18-CR-221

Count 1: 18 U.S.C. § 371
Conspiracy to commit computer fraud and related activity

Count 2: 18 U.S.C. § 1349
Conspiracy to commit wire fraud

Counts 3-11: 18 U.S.C. § 1028A
Aggravated Identity Theft

INDICTMENT

MAY 2018 Term at Alexandria, Virginia

THE GRAND JURY CHARGES THAT:

General Allegations

At all times relevant to this Indictment:

1. AHMAD 'UMAR AGHA ("AGHA") was a resident of Damascus, Syria. AGHA used the online alias, "The PRO."

2. FIRAS DARDAR ("DARDAR") was a resident of Homs, Syria. DARDAR used the online alias, "The Shadow."

3. "Spearphishing" was a term of art used to describe the act of attempting to acquire a specific person's or company's information, such as usernames, passwords, and other

identifying information, by masquerading as a trustworthy entity in an electronic communication. Perpetrators of spearphishing campaigns generally gathered background information about their target and incorporated it into the ruse to increase their likelihood of success.

COUNT 1
18 U.S.C. § 371
(Conspiracy to commit computer fraud and related activity)

THE GRAND JURY CHARGES THAT:

4. The Grand Jury realleges and incorporates by reference the factual allegations in Paragraphs 1 through 3 of this Indictment.

5. From on or about August 24, 2011 to on or about January 31, 2014, in the Eastern District of Virginia and elsewhere,

AHMAD 'UMAR AGHA,
a/k/a, "THE PRO,"

and

FIRAS DARDAR,
a/k/a, "THE SHADOW,"

and others, both known and unknown to the grand jury, knowingly and willfully conspired to commit offenses against the United States, that is:

a. Knowingly causing the transmission of programs, information, codes, or commands, in the Eastern District of Virginia and elsewhere, and as a result of such conduct, to cause damage without authorization to protected computers, and where the offense did cause and would, if completed, have caused, loss aggregating $5,000 in value to at least one person during a one-year period from a related course of conduct affecting a protected computer, damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security, and damage affecting at least 10 protected computers during a one-year period, in violation of 18 U.S.C. § 1030(a)(5)(A) and 1030(c)(4)(B);

b. Intentionally accessing a computer without authorization and thereby

obtaining information for the purpose of commercial advantage or private financial gain, in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States, and the value of the information to be obtained exceeds $5,000, in violation of 18 U.S.C. § 1030(a)(2) and 1030(c)(2)(B);

c. Intentionally conveying false and misleading information under circumstances where such information may reasonably have been believed, indicating that an activity had taken place that would have constituted a violation of 18 U.S.C. Chapters 113B, in violation of 18 U.S.C. § 1038(a)(1); and

d. Advising, counseling, urging, and causing and attempting to cause insubordination, disloyalty, mutiny, or refusal of duty by a member of the military and naval forces of the United States, and distributing and attempting to distribute written and printed matter which advised, counseled, and urged insubordination, disloyalty, mutiny, or refusal of duty by any member of the military or naval forces of the United States, with intent to interfere with, impair, and influence the loyalty, morale, and discipline of the military and naval forces of the United States, in violation of 18 U.S.C. § 2387.

Manner and Means of the Conspiracy

It was part of the conspiracy that:

6. The members of the Conspiracy agreed, combined, and worked together with each other and others to operate as an online hacking group known as the SYRIAN ELECTRONIC ARMY (hereinafter "the SEA" or "the Conspiracy").

7. As set forth in further detail below, the SEA conducted unauthorized computer intrusions in order to, among other things, spread propaganda supporting the regime of Bashar al-Assad, the President of Syria, and to retaliate against people and institutions who had been

critical of the Assad regime.

8. The general method used by the SEA to infiltrate computer systems was as follows:

a. A member of the SEA obtained email addresses for persons associated with a target entity.

b. A member of the Conspiracy sent a spearphishing email purporting to be from a trusted source that contained a link to a website which appeared to be a trusted website, but was actually controlled by the SEA.

c. Any user that clicked on the link was asked for credentials, such as a username and password, for a legitimate computer system or accounts. In a successful spearphish, at least one user provided their credentials, which the conspiracy-controlled website automatically emailed to an SEA member.

d. A member of the SEA then used the legitimate credentials without authorization to access the computer systems or accounts of the target entity.

e. Once the SEA accessed the target entity's computer systems or account, a member redirected legitimate traffic, defaced and altered text, sent messages using compromised social media and email accounts, attempted further phishing campaigns, and engaged in other unauthorized activities.

Overt Acts

9. Members of the Conspiracy committed the following overt acts in furtherance of the Conspiracy, in the Eastern District of Virginia and elsewhere:

a. In September 2011, the SEA altered the Harvard University website homepage by adding an image of Syrian President Bashar al Assad with a message saying "Syrian Electronic Army Were Here."

b. On or about October 19, 2011, the SEA used the credentials of an employee of the Washington Post, a daily newspaper based in Washington, D.C., to access, without authorization, a computer server used by the Washington Post and create a false post on its website live.washingtonpost.com.

c. On or about June 5, 2012, the SEA sent spearphishing emails to employees of the Executive Office of the President (EOP) using accounts whitehouse-online@hotmail.com and Whitehouse_online@hotmail.com. The emails contained links to sites controlled by the Conspiracy meant to harvest unsuspecting targets' EOP login credentials.

d. In August 2012, the SEA compromised the Twitter account of the Reuters news agency, an international news organization based in London, United Kingdom, and used it to send tweets with false information on the conflict in Syria. About the same time, the SEA also gained unauthorized access to the Reuters news website and published a false report in a journalist's blog.

e. On or about February 22, 2013, the SEA sent spearphishing emails to the accounts of at least two employees of the Washington Post. The Washington Post's email servers were located in the Eastern District of Virginia. The email purported to contain a link to a statement from the Government of Qatar, but it actually linked to a website controlled by the SEA. At least one Washington Post employee clicked on the link and subsequently entered his or her username and password for the Washington Post email domain.

f. On or about March 17, 2013, the SEA sent a spearphishing email to several employees of Human Rights Watch ("HRW"), a non-governmental organization

headquartered in New York, New York. The email contained a link appearing to be to a press release from the Government of Qatar, but it actually linked to an SEA-controlled website. At least five of the targeted HRW employees clicked on the link and subsequently entered their login credentials for the HRW domain. The SEA used the stolen credentials to access the HRW website without authorization and deface it with messages criticizing HRW's reports on human rights abuses by Assad regime. The SEA also used its access to the HRW email domain to send more than 6000 additional spearphishing messages to numerous victims including media organizations.

g. On or about April 15, 2013, the SEA used a real, albeit compromised, email account on the unhcr.org domain, which is used by the United Nations Refugee Agency, to send spearphishing messages to employees of National Public Radio ("NPR"), a non-profit organization that syndicates a network of approximately 900 public radio stations in the United States. As a result, the SEA obtained the usernames and passwords of more than 40 NPR employees.

h. On or about April 16, 2013, the SEA used the stolen NPR employee credentials to (i) access the NPR website without authorization, and deface several news stories; (ii) access several NPR Twitter accounts and change the passwords on those accounts; and (iii) access the NPR employees' email accounts to send additional spearphishing emails to other NPR employees.

i. On or about April 23, 2013, the SEA sent a spearphishing email from a compromised unhcr.org email account to employees of the Associated Press ("AP"). The ruse caused at least one AP employee to click on a malicious link in the email and enter his or her login credentials for the AP server into an SEA-controlled website. The SEA

used these credentials to access the AP Twitter account without authorization and change the password for the Twitter account. The SEA also used the Twitter account to post a message falsely claiming that there were two explosions in the White House and that Barack Obama had been injured.

j. On or about May 4, 2013, the SEA used a spearphishing email to obtain the login credentials for the Twitter account belonging to the entertainment channel E! Online. Without authorization, the conspirators used the account to post false information about the Syrian conflict.

k. On or about May 4, 2013, a member of the conspiracy sent an email with the subject line "theonion" from the account sea.the.shadow@gmail.com to the account th3pr0123@gmail.com that contained a list of over 25 email addresses with a domain of theonion.com.

l. On or about May 4, 2013, the SEA sent a spearphishing email appearing to be from an unhcr.org email address to employees of The Onion, a Chicago, Illinois-based satire website. The email contained a link appearing to resolve to a news article that actually resolved to an SEA-controlled website. The ruse caused at least one Onion employee to enter his or her login credentials into the Conspiracy-controlled website.

m. On or about May 6, 2013, the SEA used these credentials to gain unauthorized access to and control of the Onion employee's email account, and the conspirators further used the account to send another spearphishing email to additional Onion employees containing another fraudulent link disguised as a news article. The second spearphishing email caused at least four other Onion employees to click on the disguised link and provide their login credentials on a Conspiracy-controlled website.

n. On or about May 6, 2013, the SEA used an Onion employee's compromised email account to send a spearphishing email to additional Onion employees. The third spearphishing email replicated an earlier, legitimate email sent by the management of the Onion warning its employee about the SEA's activities and prompting them to change their passwords. The third spearphishing message contained a link purporting to resolve to a password-reset webpage, but that actually resolved to an SEA-controlled website. The ruse caused at least two Onion employees to click on the fraudulent link and enter their login credentials into the Conspiracy-controlled website. One of the victims of the third spearphishing message had administrative access to the electronic accounts of The Onion. The SEA used this victim's personal credentials to change the victim's password, and the administrative access to change the password to The Onion's Twitter accounts. Without authorization, the conspirators posted false information to Twitter using the Onion's account.

o. On or about May 15, 2013, the SEA sent a spearphishing email from a compromised account to at least one employee of the Cable News Network ("CNN"). The email contained a link that appeared to resolve to a news article but that actually resolved to a website controlled by the SEA.

p. On or about May 17, 2013, DARDAR sent an email with a subject line of "nytimes" from the account sea.the.shadow@gmail.com to the account th3pr0123@gmail.com containing a list of over 25 email addresses with a domain of nytimes.com.

q. On or about May 20, 2013, the SEA sent another spearphishing email to several additional CNN employees. The email contained a link that appeared to resolve

to a news article but that actually resolved to an SEA-controlled website. The ruse caused several CNN employees to click on the link and enter their usernames and passwords into the Conspiracy-controlled website.

r. On May 20, 2013, DARDAR sent an email from the account sea.the.shadow@gmail.com to the account th3pr0123@gmail.com. The email contained a list of usernames at CNN.

s. On or about July 26, 2013, the SEA created an email account that appeared to belong to a known employee of the EOP. It used the account to send spearphishing emails to the personal and work email addresses of several other EOP employees. The emails contained a link that appeared to resolve to media websites but that actually resolved to an SEA-controlled website. The ruse caused at least one EOP employee, VICTIM 1, to click on a link and provide his or her credentials. The SEA used these credentials to gain unauthorized access to the employee's personal email account, adjust the account settings to automatically forward incoming emails to an SEA-controlled email account, and send spearphishing emails to other EOP employees, at least one of which requested the password for a White House social media account.

t. In or around July 2013, the SEA gained unauthorized access to the website of the Daily Dot, where they deleted a legitimate article about Syria and defaced the site with images related to Syria.

u. On or about August 13, 2013, the SEA sent spearphishing emails to a number of sports journalists, including to J.R., a writer at the Washington Post. The spearphishing emails appeared to resolve to legitimate websites, but actually directed victims to an SEA-controlled website. Using this fraudulent scheme, members of the

SEA obtained J.R.'s credentials to online accounts, and they used J.R.'s credentials to access and post to J.R.'s Twitter account without authorization.

v. On or about August 14, 2013, the SEA sent spearphishing emails disguised to look as though they came from the Chief Executive Officer of Outbrain, Inc., to numerous Outbrain employees. The spearphishing emails contained a link that appeared to resolve to a media website but that actually resolved to an SEA-controlled website. The ruse caused at least one employee of Outbrain to click on the link and provide his or her email credentials.

w. On or about August 15, 2013, the SEA used the Outbrain employee's credentials to obtain unauthorized access to Outbrain's advertising controls. The conspirators used the advertising controls to redirect web traffic for a number of Outbrain's customers, including CNN, The Washington Post, and Time.

x. On or about August 19, 2013, the SEA created an email account disguised to look as though it belonged to the Chief Executive Officer of Chartbeat, Inc., a media analytics company. Members of the conspiracy used the account to send emails to Chartbeat employees containing a link that appeared to resolve to a media website, but that actually resolved to an SEA-controlled website. The ruse caused at least one Chartbeat employee to click on the link and provide his or her email credentials.

y. On or about August 19, 2013, the SEA sent at least one additional spearphishing email to other Chartbeat employees in an attempt to induce them to click on other malicious links.

z. On or about August 19, 2013, the SEA used credentials it obtained via one of its spearphishing emails to Chartbeat employees to obtain unauthorized access to an

employee's email account. That account contained the password for Chartbeat's Twitter account.

aa. On or about August 21, 2013, members of the conspiracy used this password to gain unauthorized access to Chartbeat's Twitter account, where they posted the SEA logo.

bb. Also on or about August 21, 2013, the SEA used login credentials fraudulently obtained from a Chartbeat employee to reset the password to a Chartbeat administrator account and access Chartbeat's internal computer systems.

cc. On or about August 20, 2013, the SEA sent spearphishing emails disguised to look like those from a Gannett employee to several other Gannett employees. The spearphishing emails contained a link that appeared to resolve to a news article, but actually resolved to an SEA-controlled website.

dd. Also on or about August 20, 2013, the SEA sent spearphishing emails disguised to look as though they came from a USA Today employee, to several other USA Today employees. The spearphishing emails contained a link appearing to resolve to a media website that actually resolved to an SEA-controlled website.

ee. On or about August 23, 2013, the SEA sent numerous spearphishing emails disguised to appear as if they came from the Chief Executive Officer of Melbourne IT, an Australian internet company, to several Melbourne IT employees. The emails contained a link that appeared to resolve to a media website but that actually resolved to an SEA-controlled website. At least two Melbourne IT employees clicked on the link and entered their Melbourne IT system login credentials. The Conspiracy used the credentials to gain unauthorized access to Melbourne IT's computer systems and

access Melbourne IT's business information. The Conspiracy also used the credentials to access Domain Name Service tables otherwise controlled by Melbourne IT, and to redirect numerous website domains of Melbourne IT customers to an SEA-controlled website. The redirected domain names included "huffingtonpost.co.uk" and "nytimes.com."

ff. On or about August 12, 2013, members of the SEA used a spearphishing email to obtain the login credentials for multiple New York Post Twitter accounts, and they further used their unauthorized access to post pro-Syrian Government messages on these accounts.

gg. On or about September 1, 2013, the SEA sent a spearphishing email disguised to as though it came from the Chief Executive Officer of J. Walter Thompson, a marketing communications company, to a company employee. The email contained a link appearing to resolve to a media website that actually resolved to an SEA-controlled website. The ruse caused the employee to click on the link and enter his or her login credentials. The SEA used its unauthorized access to the employee's email account to access and reset the password for an associated Network Solutions account. The SEA also deleted an email evidencing the intrusion into the Network Solutions account from the victim employee's email account, and altered the email account settings to automatically forward incoming emails to an SEA-controlled email account.

hh. On or about September 2, 2013, the SEA used the unauthorized access to the Network Solutions account to redirect the domain www.marines.com, a website used by the United States Marine Corps for the recruitment of new enlistees and officer candidates, to an SEA-controlled website. The SEA-controlled website contained a

message that encouraged potential enlistees and officer candidates to "refuse [their] orders," and invited them to fight alongside the Syrian Army.

ii. On or about September 20, 2013, the SEA sent a spearphishing email appearing to originate from a NASA employee to several other NASA employees, including some at Langley Research Center in Hampton, Virginia, in the Eastern District of Virginia. The spearphishing email contained a link appearing to resolve to a news article that actually resolved to an SEA-controlled website. At least four NASA employees clicked on the link, but their access to the SEA-controlled site was thwarted by NASA network security devices.

jj. On or about November 8, 2013, the SEA used a spearphishing email to obtain the email login credentials for D.P., an employee of Vice Media, a media company. The SEA used these credentials to deface Vice.com and redirect its traffic to an SEA-controlled website. Vice.com was hosted on a server located in the Eastern District of Virginia.

kk. On or about November 12, 2013, the SEA used a spearphishing email to obtain the email and Twitter credentials of a filmmaker who had been critical of the Syrian government. The SEA used these credentials to deface the filmmaker's website and Twitter account, and obtain copies of his personal correspondence.

ll. On or about November 29, 2013, the SEA used a spearphishing email to obtain the email credentials of a Time Magazine employee. The Conspiracy used the credentials to obtain unauthorized access to, and deface, the Time Magazine Twitter account and an online poll.

mm. In or around January 2014, the SEA used a spearphishing email to obtain

the email login credentials of several Microsoft employees. The Conspiracy used the credentials to gain unauthorized access to a Microsoft blog and Twitter account.

(All in violation of 18 U.S.C. § 371)

COUNT 2
18 U.S.C. § 1349
(Conspiracy to commit wire fraud)

THE GRAND JURY FURTHER CHARGES THAT:

10. The Grand Jury realleges and incorporates by reference the factual allegations in Paragraphs 1 through 9 of this Indictment and further charges that:

11. From on or about August 24, 2011 to on or about January 31, 2014, in the Eastern District of Virginia and elsewhere,

AHMAD 'UMAR AGHA,
a/k/a, "THE PRO,"

and

FIRAS DARDAR,
a/k/a, "THE SHADOW,"

and others, both known and unknown to the grand jury, conspired to devise a scheme and artifice to defraud and obtain property from victims entities and individuals by means of materially false and fraudulent pretenses, representations, and promises, and did knowingly transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, writings, sign, signals, pictures, and sounds, namely transmitting electronic messages containing instructions meant to deceive users of their origin and purpose, electronic messages containing illicitly obtained credentials (including usernames and passwords), and additional fraudulent messages for the purpose of executing and attempting to execute the scheme and artifice.

Manner and Means of the Conspiracy

It was part of the conspiracy that:

12. The members of the Conspiracy agreed, combined, and worked together with each other and others, known and unknown to the grand jury, to operate as an online hacking

group known as the SYRIAN ELECTRONIC ARMY (also known as "the SEA" or "the Conspiracy").

13. As set forth in further detail below, the SEA in Syria sent fraudulent electronic messages to persons in the United States, including residents of the Eastern District of Virginia, meant to deceive those persons of their origin and purpose.

14. The general method used by the SEA as part of its fraudulent scheme can be summarized as follows:

a. A member of the SEA obtained email addresses for persons associated with a target entity.

b. A member of the Conspiracy sent a spearphishing email purporting to be from a trusted source that contained a link to a website which appeared to be a trusted website, but that was actually controlled by the SEA.

c. Any user that clicked on the link was asked for credentials, such as a username and password, for a legitimate computer system or accounts. In a successful spearphish, at least one user provided their credentials, which the conspiracy-controlled website automatically sent as an electronic message to an SEA member.

d. A member of the SEA then used the legitimate credentials without authorization to access the computer systems or accounts of the target entity and caused fraudulent messages to be sent from that account.

e. Once the SEA accessed the target entity's computer systems or account, a member redirected legitimate traffic, defaced and altered text, sent messages using compromised social media and email accounts, attempted further phishing campaigns, and engaged in other unauthorized activities.

15. The members of the Conspiracy together devised a scheme whereby a member of the conspiracy would gain unauthorized access to a victim entity's or individual's computer system or accounts, among other means, by sending spearphishing emails that allowed them to ultimately steal information and employ usernames and passwords. In some instances, the members of the Conspiracy conspired to use such access to obtain further property and information.

Overt Acts

16. Members of the Conspiracy committed the following overt acts in furtherance of the Conspiracy, in the Eastern District of Virginia and elsewhere:

a. On or about February 22, 2013, a member of the Conspiracy sought and obtained information from an employee of the Washington Post using electronic communications which appeared to be from mos-office@mofa.gov.qa.

b. On or about March 17, 2013, a member of the Conspiracy sought and obtained information from an employee of Human Rights Watch using electronic communications which appeared to be from mos-office@mofa.gov.qa.

c. On or about March 17, 2013, a member of the Conspiracy sought and obtained information from an employee of Human Rights Watch using electronic communications from a compromised hrw.org account.

d. On or about April 15, 2013, a member of the Conspiracy sought and obtained information from an employee of National Public Radio using electronic communications from a compromised unhcr.org account.

e. On or about April 23, 2013, a member of the Conspiracy sought and obtained information from an employee of Associated Press using electronic

communications from a compromised unhcr.org account.

f. On or about May 4, 2013, a member of the Conspiracy sought and obtained information from an employee of The Onion using electronic communications from a compromised unhcr.org account.

g. On or about May 6, 2013, a member of the Conspiracy sought and obtained information from employees of The Onion using electronic communications from at least one compromised The Onion account.

h. On or about May 14, 2013, a member of the Conspiracy sought and obtained information from D.A., an employee of CNN, using electronic communications from the compromised account of another media organization.

i. On or about May 20, 2013, a member of the Conspiracy sought and obtained information from C.R., an employee of CNN, using electronic communications from multiple compromised electronic accounts of another media organization.

j. On or about July 26, 2013, a member of the Conspiracy sought and obtained information from an employee of the Executive Office of the President using electronic communications from the compromised personal email account of a colleague.

k. On or about July 27, 2013, a member of the Conspiracy sought and obtained information from an employee of the EOP using electronic communications from the compromised personal email account of a colleague.

l. On or about July 27, 2013, a member of the Conspiracy sought the password to a White House social media account from employees of the EOP using electronic communications from the compromised personal email account of a colleague.

m. On or about August 13, 2013, a member of the Conspiracy sought and

obtained information from J.R., a writer at the Washington Post, using electronic communications that appeared to come from another Washington Post employee.

n. On or about August 14, 2013, a member of the Conspiracy sought and obtained information from an employee of Outbrain using electronic communications that appeared to come from the Chief Executive Officer of Outbrain.

o. On or about August 19, 2013, a member of the Conspiracy sought and obtained information from an employee of Chartbeat using electronic communications that appeared to come from the Chief Executive Officer of Chartbeat.

p. On or about August 20, 2013, a member of the Conspiracy sought and obtained information from an employee of Gannett using electronic communications that appeared to come from a fellow Gannett employee.

q. On or about August 20, 2013, a member of the Conspiracy sought and obtained information from an employee of USA Today using electronic communications that appeared to come from a fellow USA Today employee.

r. On or about August 23, 2013, a member of the Conspiracy sought and obtained information from an employee of Melbourne IT using electronic communications that appeared to come from the Chief Executive Officer of Melbourne IT.

s. On or about September 1, 2013, a member of the Conspiracy sought and obtained information from an employee of J. Walter Thompson using electronic communications that appeared to come from the Chief Executive Officer of J. Walter Thompson.

t. On or about September 20, 2013, a member of the Conspiracy sought and

obtained information from National Aeronautics and Space Administration employees using electronic communications that appeared to come from fellow NASA employees.

u. On or about November 8, 2013, a member of the Conspiracy sought and obtained information from an employee of Vice Media using electronic communications that appeared to come from the Chief Technology Officer of Vice Media.

(All in violation of Title 18, United States Code, Section 1349).

COUNTS 3-11
18 U.S.C. § 1028A
(Aggravated Identity Theft)

THE GRAND JURY FURTHER CHARGES THAT:

17. The Grand Jury realleges and incorporates by reference the factual allegations in Paragraphs 1 through 9 of this Indictment into each of Counts 3-11 and further charges that:

18. On or about the dates specified in each Count below in the Eastern District of Virginia and elsewhere,

AHMAD 'UMAR AGHA,
a/k/a, "THE PRO,"

and

FIRAS DARDAR,
a/k/a, "THE SHADOW,"

did knowingly transfer, possess, and use, without lawful authority, or aid and abet in the transfer, possession, and use of, a means of identification of another person during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), that is Conspiracy to Commit Wire Fraud in violation of 18 U.S.C. § 1349, knowing that the means of identification belonged to another actual person. The allegations for each predicate felony count specified below are hereby incorporated into Counts 3-11.

COUNT	DATE	ACTUAL PERSON TO WHOM THE MEANS OF IDENTIFICATION BELONGED
3	May 20, 2013	D.A., an employee of CNN
4	May 20, 2013	C.R., an employee of CNN
5	July 27, 2013	E.L. (VICTIM 1)
6	August 13, 2013	J.R., a writer at the Washington Post
7	August 14, 2013	S.Z., an employee of Outbrain
8	August 19, 2013	J.S., an employee of Chartbeat
9	August 23, 2013	G.E., an employee of Melbourne IT
10	September 1, 2013	M.P., an employee of J. Walter Thompson
11	November 8, 2013	D.P., a Vice employee

(All in violation of Title 18, United States Code, Section 1028A(a)(1) and 2)

A TRUE BILL:

Pursuant to the E-Government Act, the original of this page has been filed under seal in the Clerk's Office.

Foreperson of the Grand Jury

TRACY DOHERTY-MCCORMICK
ACTING UNITED STATES ATTORNEY

Jay V. Prabhu
Maya D. Song
Assistant United States Attorneys

JOHN C. DEMERS
ASSISTANT ATTORNEY GENERAL
NATIONAL SECURITY DIVISION

Nathan Charles
Scott McCulloch
Trial Attorneys